



December 21, 2018

TO: David S. Ferriero
Archivist of the United States

FROM: James Springs *James Springs*
Inspector General

SUBJECT: *Audit of National Archives and Records Administration's Compliance with the Federal Information Security Modernization Act*
Audit Report No. 19-AUD-02

This memorandum transmits the results of the final report for the *Audit of National Archives and Records Administration's Compliance with the Federal Information Security Modernization Act*. It also transmits *Management's Response* and the *Office of Inspector General's Assessment of Management's Response and Proposed Actions* to the report (see page 56).

We contracted with independent certified public accounting firm CliftonLarsonAllen LLP (CLA) to audit National Archives and Records Administration's (NARA) compliance with the Compliance with the Federal Information Security Modernization Act of 2014. The contract required the audit be performed in accordance with generally accepted government auditing standards (GAGAS). CLA is responsible for the attached report dated December 14, 2018, and the results expressed in the accompanying report. To ensure the quality of their work performed, we evaluated the independence, objectivity, and qualifications of the staff; reviewed the audit plan and approach of the audit; monitored the performance of the audit; reviewed CLA's report and related documentation; and inquired of its representatives. Our review disclosed no instances where CLA did not comply, in all material aspects, with GAGAS.

The report contains 27 recommendations, which are intended to strengthen NARA's information security program. Your office concurred with all of the recommendations. Based on your December 19, 2018 response to the final draft report, we consider all recommendations resolved and open. Once your office has fully implemented the recommendations, please submit evidence of completion of agreed upon corrective actions so that recommendations may be closed.

As with all OIG products, we determine what information is publically posted on our website from the attached report. Consistent with our responsibility under the *Inspector General Act, as amended*, we may provide copies of our report to congressional committees with oversight responsibility over the National Archives and Records Administration.

We appreciate the cooperation and assistance NARA extended to us during the audit. Please call me or Jewel Butler, Assistant Inspector General for Audits, with any questions.

Attachments

cc: Debra Wall, Deputy Archivist of the United States
William Bosanko, Chief Operating Officer
Chris Naylor, Deputy Chief Operating Officer
Micah Cheatham, Chief of Management and Administration
Swarnali Haldar, Chief Information Officer
Kimm Richards, Accountability
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

**Audit of the National Archives and Records Administration's Compliance with the Federal
Information Security Modernization Act**

Fiscal Year 2018

Audit Report No. 19-AUD-02



CliftonLarsonAllen

CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com



CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com

December 14, 2018

James Springs, Inspector General
National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740

Dear Mr. Springs:

CliftonLarsonAllen LLP is pleased to present our report on the National Archives and Records Administration's (NARA) compliance with the Federal Information Security Modernization Act of 2014 (FISMA).

We appreciate the assistance we received from the staff of NARA and appreciate the opportunity to serve you. We will be pleased to discuss any questions you may have.

Very truly yours,

A handwritten signature in black ink, appearing to read 'S. Mirzakhani', is written over a light blue horizontal line.

Sarah Mirzakhani, CISA
Principal



CliftonLarsonAllen LLP
CLAAconnect.com

Inspector General
National Archives and Records Administration

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the National Archives and Records Administration's (NARA) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether NARA implemented an effective information security program in accordance with federal requirements and guidelines. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls for a sample of ten NARA internal and external information systems. We performed audit fieldwork at the NARA's facility in College Park, MD, from June 18, 2018 to December 12, 2018.

The audit was conducted in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*, issued by the Comptroller General of the United States. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We concluded that NARA did not implement an effective information security program for many of the selected security controls for selected information systems. NARA's implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in all eight Inspector General (IG) FISMA Metric Domains and have made 27 recommendations to assist NARA in strengthening its information security program.

Additional information on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP

A stylized, cursive signature of 'CliftonLarsonAllen LLP' in dark blue ink.

Arlington, Virginia
December 14, 2018

Table of Contents

- Background** 1
- Audit Methodology and Requirements** 5
- Summary of Results** 6
- FISMA Audit Results** 10
 - 1. NARA Must Strengthen its Agency-wide Information Security Program 10
 - 2. NARA Must Improve System Inventory Listing Controls 16
 - 3. NARA Must Strengthen its Process for the Review and Approval of Policy and Procedures 18
 - 4. NARA Must Provide ISSOs for Information Systems 19
 - 5. NARA Must Strengthen Configuration Management Controls 20
 - 6. NARA Must Enhance its Baseline Configuration Process 21
 - 7. NARA Must Improve its Vulnerability and Patch Management Controls 22
 - 8. NARA Must Fully Implement Multi-Factor Authentication 25
 - 9. NARA Must Strengthen Account Management Controls 26
 - 10. NARA Must Enforce Elevated Security Training 28
 - 11. NARA Must Consistently Implement Audit Logging Procedures 30
 - 12. NARA Must Strengthen Password Policies and Shared Account Management 31
 - 13. NARA Must Report Security Incidents in a Timely Manner 33
 - 14. NARA Must Develop, Maintain, and Test Contingency Plans 34
- Appendix I – Scope and Methodology** 37
- Appendix II – Acronyms** 39
- Appendix III – Management Response** 41
- Appendix IV - Summary of Results of Each Control Reviewed** 42
- Appendix V – Report Distribution List** 48

NOTE: Information has been redacted from this report that could reasonably lead to the compromise of NARA's Information Technology systems.

Background

Agency Overview

NARA is an independent agency within the executive branch of the Federal Government responsible for preserving, protecting and providing access to the records of our Government. NARA has approximately 2,800 full time equivalents (FTEs) and an operating expense appropriation of \$384.9 million in Fiscal Year (FY) 2018. NARA's facility located in College Park, Maryland. NARA has three other facilities in the Washington, D.C. area, 20 regional archives and/or Federal records centers, and 14 Presidential Libraries around the country.

Information Technology Overview

NARA relies on information technology (IT) systems to accomplish its mission of providing public access to the records of our Government. The Agency has a FISMA-reportable information systems portfolio encompassing approximately¹ 60 systems hosted both internally and externally. These systems are rated from low to high risk of impact to NARA's mission, as rated under Federal Information Processing Standards (FIPS).

NARA's Information Services office is led by the Executive for Information Services/Chief Information Officer (CIO). Information Services is responsible for NARA's nationwide information and telecommunications infrastructure and NARA information systems. The Office oversees NARA's IT security; and manages NARA's IT management processes and IT governance boards. The office also includes NARA's Chief Technology Officer, as well as a Quality Assurance Division.

NARA establishes specific organization-defined IT security policies, procedures, and parameters in its Cybersecurity Controls Family document, which incorporates the requirements of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

FISMA Legislation

FISMA² provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

¹ The total system count was based upon the FISMA inventory reviewed; however, as noted within finding number 2, missing or inaccurate information within this inventory was reported. As a result, the total count was deemed "approximate."

² The Federal Information Security Modernization Act of 2014 (Public Law 113-283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to Office of Management and Budget (OMB) and to congressional committees on the effectiveness of their information security program.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. As specified in FISMA, the agency CIO or senior official is responsible for overseeing the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires agency Office of Inspectors General (OIG) to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued the FIPS to establish agency baseline security requirements.

FY 2018 IG FISMA Reporting Metrics

OMB and the Department of Homeland Security (DHS) provide annual instructions to Federal agencies and OIGs for preparing FISMA reports. On October 16, 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*. The memorandum establishes information security priorities, and provides agencies with FY 2017-2018 FISMA and Privacy Management reporting guidance and deadlines. Accordingly, the *FY 2018 Inspector General (IG) Federal Information Security Modernization Act of 2014 Reporting Metrics* (metrics), provide IGs with reporting requirements to address a variety of attributes in five security domains in their independent assessment of agencies' information security programs.

The FY 2018 metrics are based on a maturity model approach, which aligns with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover, as highlighted in **Table 1**. Data Protection and Privacy was added to the FY 2018 metrics in the Protect security function. The Cybersecurity Framework (CSF) provides agencies with a common structure to identify and manage agency-wide cybersecurity risks, while it provides OIGs with a method to assess the maturity of agency controls that are in place to address those risks, as highlighted in **Table 1**.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2018 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains	Definitions of Core Security Functions
Identify	<ul style="list-style-type: none"> • Risk Management 	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect	<ul style="list-style-type: none"> • Configuration Management • Identity and Access Management • Data Protection and Privacy • Security Training 	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect	<ul style="list-style-type: none"> • Information Security Continuous Monitoring 	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	<ul style="list-style-type: none"> • Incident Response 	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover	<ul style="list-style-type: none"> • Contingency Planning 	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

OIGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound, risk-based policies and procedures, while the advanced levels capture the extent that agencies institutionalize those policies and procedures. **Table 2** explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.

Table 2: FY 2018 IG Assessment Maturity Model

Maturity Level	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

Maturity Level	Maturity Level Description
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Refer to Appendix IV - Summary of Results for Each Control Reviewed for detailed results of specific control effectiveness.

Audit Methodology and Requirements

The NARA OIG engaged CliftonLarsonAllen LLP (CLA) to conduct the required audit of NARA's information security program and practices. The objective of this audit was to assess the effectiveness of NARA's information security program in accordance with the FISMA of 2014, Public Law 113-283, the general and performance standards of the Government Accountability Office's (GAO's) *Generally Accepted Government Auditing Standards*; and applicable instructions from the OMB and DHS. In addition, the audit included inquiries, observations, inspection of documents and records, and testing of controls.

The audit included the testing of selected management, technical, and operational controls outlined in NIST Special Publication 800-53, Revision 4, for the following subset of NARA's information systems:

- NARANet³
- Order Fulfillment and Accounting System (OFAS)
- Records Center Program Billing System (RCPBS)
- Integrated Siebel Platform General Support System (ISE GSS)
- Information Security System Operation Network (ISSON)
- National Archives Catalog (NAC)
- Researcher Registration System (RRS)
- OpsPlanner
- Maximo
- Unclassified Redaction Tracking System (URTS)

In addition, the FISMA audit included an assessment of the effectiveness of all eight FY 2018 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions. See Appendix I for the detailed scope and methodology.

³ NARANet is comprised of the following components: Common Controls, Application Server, Desktop, File_Print and GSS Infrastructure

Summary of Results

Progress since FY 2017

We found NARA made the following improvements during FY 2018 throughout the domain areas, which CLA recognized in the IG metric responses as relevant and applicable:

- NARA communicated the *NARA Cybersecurity Framework Methodology* (CFM), developed in FY 2017, to agency staff during specialized security training provided to system owners and Information System Security Officers (ISSOs). However, prior to its promulgation, Information Services did not follow the approval process needed for the CFM as defined within NARA Directive 111.
- NARA procured a new contract to obtain ISSOs during the latter part of FY 2018.
- NARA updated its Enterprise Architecture documentation.

Current Results

While the aforementioned improvements were recognized, the continued emphasis on communication of formalized policies and procedures resulted in many of the metrics receiving “Ad-hoc” maturity levels. Key observations include:

- NARA’s Office of Information Services did not follow the process documented in NARA Directive 111 for developing and updating policy documents, including the CFM, which included roles and responsibilities for information systems monitoring.
- Although the CFM was in effect for FY 2018, its communication was not provided to key stakeholders until the latter part of FY 2018.
- ISSOs were not assigned to all systems under review due to contract⁴ timing during FY 2018.
- Several major applications⁵ did not undergo NARA’s security assessment and authorization process, and lacked fully developed security assessment packages and evaluations of the adequacy and effectiveness of security controls.

During the audit, CLA identified control weaknesses related to Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. **Table 4** provides additional detail regarding these noted weaknesses.

CLA’s conclusions as to the effectiveness of NARA’s IT security activities incorporate multiple sets of results, as outlined below.

⁴ Task order for ISSO Support Services, signed September 7, 2018.

⁵ OMB Circular A-130, Appendix III, defines major application as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

1. FISMA maturity scores and judgmental assessment

FISMA requires evaluators across the Federal government to respond to 67 objective questions, from which a DHS algorithm calculates a maturity score for each of five security functions. An evaluator may also make a subjective, judgmental assessment of the effectiveness of an agency’s IT security in each of eight metric domains. This opportunity allows the audit to reflect information that may not be captured by the objective assessment. CLA’s subjective assessment concluded that NARA’s IT security activities were not effective in each of the metric domains.

Table 3 below summarizes the maturity scores and judgmental results by category.

Table 3: FY 2018 NARA OIG Cybersecurity Framework Domain Ratings

Cybersecurity Framework Security Functions⁶	Calculated Maturity Level (Security Function)	Metric Domains	Calculated Maturity Level (Metric Domain)	Independent Assessor Audit
Identify	Defined (Level 2)	Risk Management	Defined (Level 2)	Not effective based on findings noted during the FY 2018 FISMA audit.
Protect	Ad Hoc (Level 1)	Configuration Management	Ad Hoc (Level 1)	Not effective based on findings noted during the FY 2018 FISMA audit.
		Identity and Access Management	Ad Hoc (Level 1)	Not effective based on findings noted during the FY 2018 FISMA audit.
		Data Protection and Privacy	Ad Hoc (Level 1)	Not effective based on findings noted during the FY 2018 FISMA audit.
		Security Training	Defined (Level 2)	Not effective based on findings noted during the FY 2018 FISMA audit.
Detect	Defined (Level 2)	Information Security Continuous Monitoring	Defined (Level 2)	Not effective based on findings noted during the FY 2018 FISMA audit.

⁶ See Table 1 and Table 2 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

Cybersecurity Framework Security Functions ⁶	Calculated Maturity Level (Security Function)	Metric Domains	Calculated Maturity Level (Metric Domain)	Independent Assessor Audit
Respond	Defined (Level 2)	Incident Response	Defined (Level 2)	Not effective based on findings noted during the FY 2018 FISMA audit.
Recover	Defined (Level 2)	Contingency Planning	Defined (Level 2)	Not effective based on findings noted during the FY 2018 FISMA audit.

2. Detailed findings

Table 4: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in the FY 2018 FISMA Assessment

Cybersecurity Framework Security Functions ⁷	FY 2018 IG FISMA Metric Domains	Weaknesses Noted in Core Security Functions FY 2018
Identify	Risk Management	Inventory listing inaccuracies (Finding 2)
		Information security program weaknesses (Finding 1)
		Issued policies and procedures without proper approval process (Finding 3)
		Lack of ISSOs for information systems (Finding 4)
Protect	Configuration Management	System changes without approval or testing (Finding 5)
		Baseline configuration process enhancement (Finding 6)
		Lack of patching and software updates (Finding 7)
	Identity and Access Management	Lack of multifactor authentication (Finding 8)
		Insufficient account management controls (Finding 9)
		Insufficient audit logging procedures (Finding 11)

⁷ See Table 1 and Table 2 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

Cybersecurity Framework Security Functions⁷	FY 2018 IG FISMA Metric Domains	Weaknesses Noted in Core Security Functions FY 2018
		Inadequate password and shared account controls (Finding 12)
	Security Training	Insufficient elevated security training (Finding 10)
Detect	Information Systems Continuous Monitoring	Information security program weaknesses (Finding 1)
Respond	Incident Response	Untimely incident reporting (Finding 13)
Recover	Contingency Planning	Insufficient development, maintenance, and testing of contingency plans (Finding 14)

Overall, CLA concluded that NARA needs to improve the effectiveness of its information security program. At present, the weaknesses CLA identified leave NARA operations and assets at risk for unauthorized access, misuse and disruption.

To address these weaknesses, CLA offered 27 recommendations to assist NARA in strengthening the effectiveness of its information security program. The detailed findings from the FISMA assessment, grouped by the Cybersecurity Framework Security Functions, are included in the next section, FISMA Audit Results.

FISMA Audit Results

Security Function: Identify

1. NARA Must Strengthen its Agency-wide Information Security Program

FY 18 FISMA IG Metric Area: *Risk Management and Information System Continuous Monitoring*

FISMA requires agencies to develop, document and implement an agency-wide information security program to provide information security for the information and information systems that support the agency's operations. NIST SP 800-53, Revision 4, organization-wide information security program management (PM) controls place an emphasis on the overall security program and are intended to enable compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

CLA found that NARA has not effectively implemented an organization-wide information security program. Specifically, CLA noted weaknesses in the following NIST 800-53 PM controls:

- Security Authorization Process
- Plan of Action and Milestone Process

Security Authorization Process:

CLA noted deficiencies in the Agency's security authorization process in the following areas:

- Authorization to Operate (ATO)
- System Security Plans (SSPs)
- Security Assessment Reports (SARs)
- Plan of Action and Milestones (POA&M)

NIST SP-800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information System: A Security Life Cycle Approach*, provides guidelines for applying the Risk Management Framework (RMF) to Federal information systems, providing the structure for the security authorization of federal information systems as follows:

- Selecting and implementing security controls for the information system and describing how the controls are implemented in the system security plan;
- Assessing whether the controls are operating as intended;
- Analyzing and assessing risk to the information system based on weaknesses and vulnerabilities identified; and
- Authorizing the information system based on the determination of risk.

Authorization to Operate

NARA did not maintain current system ATOs for some of the information systems in our sample. Specifically, the ISSON, Maximo, and OpsPlanner systems were in operation without an ATO. The lack of ISSO continuity has hindered NARA's ability to develop, conduct, and maintain the security assessment and authorization process in accordance with FISMA requirements.

NIST SP 800-37, Glossary defines "Authorization to Operate" as follows:

"The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls."

NIST SP 800-37, Appendix F, F.1 Authorization Package states:

"The security authorization package documents the results of the security control assessment and provides the authorizing official with essential information needed to make risk based authorization decisions."

The authorization package contains the following documents: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones.

Without formally documenting an information system's authorization to operate, the NARA Authorizing Official (AO) has not accepted the risk, which diminishes NARA's ability to hold AOs accountable for their information systems. Further, the security posture of NARA systems may not have an acceptable level of risk to operate, exposing NARA to unmitigated security risk, potentially compromising Agency information or information systems.

System Security Plans

The purpose of a system security plan is to describe the information system, including the system boundary, and document the security controls both planned and implemented for the system. Although NARA has an *Information System Security Officer Guide*, which establishes procedures to review and update SSPs and other security documentation, NARA did not maintain accurate and up-to-date system security plans for all its information systems.

Specifically, CLA identified the following weaknesses in system security plan management:

- SSPs were not developed for the following systems:
 - ISE GSS
 - OpsPlanner
 - Maximo
- SSPs were not updated to reflect all NIST SP 800-53, Revision 4 privacy controls for the following systems:
 - RRS
 - OFAS
 - NAC
 - URTS
 - NARANet

- Control implementation details were missing for the following systems:
 - NARANet Common Controls
 - NARANet Desktop
 - NARANet Infrastructure
 - OFAS
 - RCPBS
 - ISSON
 - URTS

- SSPs were missing specific content, such as authorization boundary, operational context of the system, overview of the security requirement for the system, and approval by the authorizing official for the following systems:
 - NARANet GSS Common Controls
 - NARANet Application Servers
 - NARANet Desktops
 - NARANet File and Print server
 - NARANet Infrastructure
 - OFAS
 - ISSON
 - RRS
 - URTS

Although Information Services was in the process of updating system security plans that were determined incomplete, this effort was unfinished as of the end of FY 2018. The lack of ISSO continuity has hindered NARA's process to develop and maintain SSPs, which are part of the ISSO's responsibilities.⁸

NIST SP 800-37, Appendix F, F.1 Authorization Package states the following:

“The security plan, prepared by the information system owner or common control provider, provides an overview of the security requirements and describes the security controls in place or planned for meeting those requirements. The plan provides sufficient information to understand the intended or actual implementation of each security control employed within or inherited by the information system.”

Without complete and up to date SSPs, developed in accordance with NARA IT Security Requirements, there is a risk that NARA systems will be susceptible to new security threats resulting from changes in its internal and external control environment. Additionally, the CIO will not be able to place reliance on system documentation in order to make accurate security decisions.

System Assessment Reports

A system risk assessment is performed to identify risks to the Agency pertaining to the operation of NARA's information systems. When assessing risk, an analysis of known threats and vulnerabilities should be considered. In addition, when agencies use systems owned and operated

⁸ NARA procured a new contract to obtain ISSOs during the latter part of FY 2018.

by external parties, it is necessary to ensure that external service providers employ adequate security controls in order to protect the agency's data.

NARA did not adequately assess system risks. Specifically, CLA identified the following system risk assessments that did not consider all known system risks:

- The risk assessment for NAC was last updated in 2014, instead of on an annual basis.
- The SAR for the NARANet, RRS and NAC systems did not identify a summary of test failures for all failed controls. In addition, the SAR for the RCPBS, RRS and OFAS systems did not list recommended countermeasures for all failed controls.

NIST SP 800-53, Revision 4, security control RA-3, Risk Assessment, states:

“The organization:

- a) conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.”

The *NARA IT Security Methodology*, under CA-2 Security Assessments, requires the development of a security assessment plan, which describes the scope of the assessment, security controls and control enhancements under assessment, assessment procedures to be used to determine security control effectiveness; and the assessment environment, assessment team, and assessment roles and responsibilities.

The *NARA Cybersecurity Framework Methodology*, under Task 4.2: Update Risk Assessment, states:

“Risk assessment are updated annually or whenever there are significant changes to the information system or environment of operations (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.”

The lack of ISSO continuity has also hindered NARA's ability to develop, conduct, and maintain the security assessment and authorization process in accordance with FISMA requirements.

Without assessing the operating effectiveness of security controls, the CIO does not have assurance that system controls are operating effectively, which may expose critical systems to information loss or abuse. In addition, without an accurate depiction of the current and applicable security weaknesses of a system, the CIO is at risk of missing potential security risks.

Plan of Action and Milestone Process:

POA&Ms describe corrective action plans for system weaknesses noted from security control assessments, vulnerability assessments and system audits. The POA&Ms are used by the authorizing official to monitor the progress of remediation for system control weaknesses.

NARA did not follow proper POA&M management procedures for six of the systems in scope. The POA&Ms for OFAS, ISE GSS, URTS, RRS, NARANet, NAC and RCPBS either missed completion dates, dates were not indicated, or failed controls were not documented. Specifically, the following weaknesses were noted:

- POA&Ms were missing scheduled completion dates for weaknesses reported for the OFAS, ISE GSS, RRS and URTS systems.
- POA&Ms were not consistently opened for failed controls identified within SAR's for the RRS and NARANet GSS Common Controls, NARANet Common Controls, Application Servers, Desktops, File and Print servers and Infrastructure, OFAS, RCPBS, NAC and URTS systems.
- POA&Ms were not consistently opened for failed controls identified within the OFAS Risk Assessment.
- POA&Ms were not reviewed and updated during FY 2018 for RRS.
- Scheduled completion dates for POA&Ms were missed for NARANet, RRS, RCPBS and NAC systems.

Many NARA systems lacked an ISSO for the entire year. ISSOs, in coordination with the Monitoring & Authorization branch, are typically responsible for performing continuous monitoring functions such as opening and closing POA&Ms.⁹

NIST SP 800-53, Revision 4, security control CA-5, Plan of Action and Milestones, states:

“The organization:

- a) Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system;”

POA&Ms are used by the authorizing official to evaluate corrective action plans and estimated timeframes for remediation of control weaknesses, and to monitor the progress of remediation. Without the completion of POA&Ms for known control weaknesses, a plan for corrective action is delayed, leaving NARA susceptible to system security risks.

Recommendations

To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO:

Recommendation 1: Ensure complete security authorization packages for each major application and general support system¹⁰ are completed prior to deployment into production.

Management Response

NARA verbally concurs with this recommendation.

⁹ Ibid. footnote 4.

¹⁰ OMB Circular A-130, Appendix III, defines general support system as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 2: Ensure SSPs are developed for all NARA systems in accordance with NARA policy.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 3: Ensure SSPs are reviewed and updated for all NARA systems in accordance with NARA policy to ensure any missing control implementation details are completed, and missing privacy controls added.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 4: Conduct risk assessments for each system in operation and establish policies or procedures to ensure that risk assessments are conducted at least annually.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 5: Document summaries of test failures for all failed controls identified in Security Assessment Reports.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 6: Ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated timely; and are updated to include detailed information on the status of the corrective actions.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

2. NARA Must Improve System Inventory Listing Controls

FY 18 FISMA IG Metric Area: *Risk Management*

FISMA requires that agencies establish an inventory of major information systems¹¹ to support FISMA activities. The FISMA inventory is used to track security information for all systems. The NARA system inventory contained several inaccuracies and missing information, including a notation of the Maximo system as a "planned" system, despite it being active, and lack of system interconnections listed for each system.

Since Maximo was in the planning phases of being moved from a physical system to a cloud based system, management decided to incorrectly update the system inventory listing and keep the status as "planned" instead of "active;" however, the system remained in operation during the planning period. Due to a lack of management oversight, system interconnections were not described in the inventory listing. Although system interconnections may be described within system security plans, weaknesses were noted in the creation and updating of these documents for several systems, as reported in Finding Number 1.

NARA IT Security Requirements, control PM-5, information system inventory, states "For all data, the NARA Office of Information Services shall develop and maintain an inventory of its information systems."

U.S. Code Title 44 Chapter 35 Subchapter I § 3505

Inventory of Major Information Systems, states:

"(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.

¹¹ OMB Circular A-130 defines a "major information system" as an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

- (2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.”

The *NARA Cybersecurity Framework Methodology*, under Task 2.1.2: Vetting the Information Systems Inventory, states:

“The following FISMA Inventory Standard applies to all IT systems owned by NARA or operated on behalf of NARA (e.g., by a contractor):

- 1) Every GSS shall be explicitly listed in the NARA FISMA Inventory and is FISMA reportable.
- 2) Each Major Application shall be explicitly listed in the NARA FISMA Inventory and is FISMA reportable.
- 3) Each Minor Application shall be accounted for in the NARA FISMA Inventory by either explicitly listing it or by including it in the accreditation boundary of a GSS or Major Application. Any additional security controls that are specific to the Minor Application should be documented in the GSS or Major Application system security plan as an appendix or paragraph. Minor Applications that are included in the accreditation boundary of a GSS or Major Application are not FISMA reportable as they are accounted for in the SA&A of the GSS or Major Application. Minor Applications that are not included in the accreditation boundary of a GSS or Major Application are FISMA reportable.”

The lack of an accurate system inventory increases the risk of improper system accountability resulting in NARA not being fully aware of all the systems they manage and associated risks with unaccounted systems. Additionally, without a listing of interconnections, NARA may not be accounting for all external pathways into their systems.

Recommendation

To assist NARA with strengthening its system inventory controls, CLA recommends the CIO:

Recommendation 7: Ensure the system inventory listing is updated to accurately reflect NARA’s current operating environment.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA’s formal written response, we consider this recommendation unresolved and open.

3. NARA Must Strengthen its Process for the Review and Approval of Policy and Procedures

FY 18 FISMA IG Metric Area: *Risk Management*

Information security controls have been designed to facilitate compliance with applicable federal orders, directives, policies, regulations, standards, and guidelines. Within NARA, (as described within NARA Directive 111) directives consist of policy directives, supplements, and interim guidance.

- a. **Policy directives** prescribe or amend NARA internal policy, procedures, authorities, or organizational structure. These policies and procedures are necessary to accomplish the programs and functions of NARA.
- b. **Supplements** provide detailed procedures, examples, useful hints, etc., to assist employees in carrying out the policy contained in a directive. Supplements cannot contradict policy directives.
- c. **Interim guidance** provides temporary NARA internal policy, procedures, authorities, or organizational structure. Interim guidance is issued when policy must be immediately conveyed. An interim guidance should be incorporated into a policy directive within one year of the signature date.

The *NARA IT Security Methodology* (e.g., Incident Response, Access Controls, etc.), IT Security Requirements, and Cybersecurity Framework Methodology: Processes & Procedures, is considered by Information Services as a NARA IT policy supplement. However they were not formally reviewed by Strategy and Performance (formerly NPOL mentioned in NARA Directive 111) and approved by the Office Head in accordance with NARA Directive 111.

NARA Directive 111 requires specific individuals to review and approve changes to policy directives, supplements and interim guidance. Information Services was unaware policy supplements were required to be reviewed by Strategy and Performance, and has experienced ongoing delays obtaining final review of NARA Directive 804 (which the supplements were designed to support) from Strategy and Performance. Delays in the review process were further complicated given annual updates to these directives as the result of new regulations and requirements from NIST and OMB.

Specifically, NARA Directive 111 prescribes procedures for the formal review by Strategy and Performance staff prior to forwarding to the approving official for signature. In the case of policy supplements, Office Heads can perform a review; however, Strategy and Performance must review the text before issuance.

Without following proper policy and procedure approval processes, policies and procedures may not be properly developed and disseminated to key stakeholders. Additionally, it could cause confusion as to which document is the officially accepted document.

Recommendation

To assist NARA with strengthening its policy and procedure development and authorization controls, CLA recommends the Chief Information Officer in coordination with Strategy and Performance staff:

Recommendation 8: Ensure IT policies, procedures, methodologies and supplements are reviewed and approved in accordance with NARA Directive 111.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

4. NARA Must Provide ISSOs for Information Systems

FY 18 FISMA IG Metric Area: *Risk Management*

The ISSO has the responsibility to ensure the appropriate operational security posture is maintained for an IT system. An ISSO serves as a principal advisor to the Information System Owner and the Chief Information Security Officer (CISO)/Information System Security Manager (ISSM) on all matters, technical and otherwise, involving the secure configuration and maintenance of an information system.

NARA did not have ISSOs in place for all its information systems to provide adequate support and security monitoring. Specifically, the NAC, RRS, OpsPlanner, URTS, and OFAS systems did not have assigned ISSOs. NARA's ISSO contract was terminated prior to FY 2018, and the CIO did not ensure a new ISSO contract was in place for the beginning of the fiscal year.¹² There was also a funding resource constraint, which hindered the ability for NARA to obtain ISSOs for every major application and general support system.

The *NARA Information System Security Officer Guide* requires the ISSO serve as the principal advisor to the information system owner, CISO, and ISSM on all matters (technical and otherwise) involving the security of the information system.

NIST SP 800-18, Revision 1, *Guide for Developing System Security Plan for Federal Information Systems*, states:

“The information system security officer is the agency official assigned responsibility by the Senior Agency Information Security Officer (SAISO), authorizing official, management official, or

¹² Ibid. footnote 4.

information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.”

Without adequate ISSO support, there is an increased risk that security controls may not be adequately monitored and addressed to implement security requirements. There is also the risk that the CISO and System Owner will not have adequate insight into the continuous monitoring process, when making determinations for system authorizations to operate. Consequently, NARA may not be providing information security protections commensurate with the risk and magnitude resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

Recommendation

To assist NARA with strengthening its ISSO management controls, CLA recommends the CIO:

Recommendation 9: Assign ISSO’s for all major applications and general support systems.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA’s formal written response, we consider this recommendation unresolved and open.

Security Function: Protect

5. NARA Must Strengthen Configuration Management Controls

FY 18 FISMA IG Metric Area: *Configuration Management*

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

For a sample of 19 NARANet system changes (from the total population of 192 NARANet system changes), CLA noted one (1) change was not approved by management prior to implementation, and one (1) change did not have evidence of test plans and test results.

Although management asserted that NARA considers critical patches as pre-approved patches, which do not require management’s approval before implementation, NARA’s policies and procedures do not define critical patches as pre-approved patches. In addition, NARA did not maintain evidence for test plans and test results for all changes that were put into production.

NIST SP 800-53, Revision 4, security control CM-3, Configuration Control, states:

“The organization:

b. reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses

c. documents configuration change decisions associated with the information system

d. implements approved configuration-controlled changes to the information system.”

“Control enhancement

(2) The organization must test, validate, and document changes to the information system before implementing the changes on the operational system.”

Without proper change management procedures, including testing, security deficiencies and vulnerabilities may exist that go undetected. Without proper approvals, changes may be inappropriately moved into production.

Recommendation

To assist NARA with strengthening its change management controls, CLA recommends the Chief Information Officer:

Recommendation 10: Ensure that all applicable changes are tested and properly approved before being implemented into production, with evidence maintained of testing and approvals.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA’s formal written response, we consider this recommendation unresolved and open.

6. NARA Must Enhance its Baseline Configuration Process

FY 18 FISMA IG Metric Area: *Configuration Management*

Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.

The following configuration baselines were not updated or reviewed on an annual basis, in accordance with NARA IT Security Requirements:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Although configuration baselines were developed, Information Services did not consistently implement a process to ensure they were reviewed on an annual basis.

NARA IT Security Requirements, security control CM-2, for baseline configurations, states that, for data requiring moderate or high integrity, the NARA System Owner shall review and update the baseline configuration of the information system at least annually.

NARANet Common Controls System Security Plan, security control CM-2, Baseline Configuration, states:

“Per OMB requirements, NARA’s desktop computers must adhere to the United States Government Configuration Baseline (USGCB) settings. NARANet uses Policy Auditor to monitor for USGBC and [Center for Internet Security] CIS compliance. [NARA IT Telecommunications and Support Services] NITTSS/[IT Operations] IOO, jointly with [Information Services] IS, review and update baseline configurations for operating systems in the environment on an annual basis, when required due to changes to the baseline configuration, and as an integral part of component installation and upgrades.”

Without regular reviews and updates of baseline configurations, critical systems could be exploited by an attacker, allowing for a denial of service attack, or providing a mechanism for unauthorized access to files and data.

Recommendation

To assist NARA with strengthening its baseline configuration management controls, CLA recommends the CIO:

Recommendation 11: Ensure reviews of baseline configurations are performed on an annual basis and updated as necessary.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA’s formal written response, we consider this recommendation unresolved and open.

7. NARA Must Improve its Vulnerability and Patch Management Controls

FY 18 FISMA IG Metric Area: *Configuration Management*

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems, and is an important component of vulnerability management. Patches correct

security vulnerabilities and functionality problems in software. Applying patches to eliminate these vulnerabilities significantly reduces the risk of exploitation. In addition, patches are usually the most effective way to mitigate software flaw vulnerabilities, and are often the foundation for an effective vulnerability management program.

NARA did not have a process in place to remediate known patch and software updates for critical and high severity vulnerabilities in a timely manner. Specifically, we noted the following as a result of independent vulnerability scans:

- Out of a total of 3,734 hosts, we identified 176 unique vulnerabilities (comprised of 71 critical and high risk weaknesses existing on 379 hosts). Of these 379 hosts, 167 vulnerabilities (95%) were the result of missing patches. Details of specific patches missing were provided to Information Services management under separate cover, given their sensitive nature. Of the vulnerabilities related to missing patches, 165 unique vulnerabilities were publically disclosed in 2017 or earlier.
- [REDACTED]
- [REDACTED]
- The RCPBS environment has two hosts of which four unique vulnerabilities existed (comprised of one high-risk vulnerability), including the same patch was missing on each host.
- The OFAS environment has 67 hosts that have 17 unique vulnerabilities, including 3 high risk vulnerabilities. CLA identified one high-risk vulnerability for missing patches on two different hosts.

Although management had a patch and vulnerability management program in place, it was not effective to ensure all needed software patches and upgrades are implemented timely. Specifically, NARA was not proactive in ensuring that its software was running on vendor-supported versions. Software vendors announce upcoming end of service dates well in advance for their products; however, we identified instances of NARA utilizing unsupported versions of certain software. NARA planned for the Windows Server operating system migration; however, these actions did not adequately prepare NARA for the challenges and potential delays often associated with the migration of a major operating system on its servers, to ensure the migration was completed prior to the conclusion of vendor support.

NIST SP 800-53, Revision 4, security control SI-2 for flaw remediation states:

“The organization:

- a. identifies information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.”

NIST SP 800-53, Revision 4, security control SA-22 for unsupported system components, states:

“The organization:

- a. replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.”

Missing patches increase the risk of weaknesses being exploited and potential information loss or disclosure. Since the migration and upgrade process from Windows Server 2003 to a different supported vendor platform has continued beyond the July 14, 2015 end of life support date indicated by Microsoft, the risk of an attacker exploiting known vulnerabilities in Windows Server 2003 continues to increase and threatens the confidentiality, integrity and availability of those programs and data residing on those servers.

Recommendations

To assist NARA with strengthening its vulnerability management controls, CLA recommends the CIO:

Recommendation 12: Implement improved processes to remediate security deficiencies on NARA’s network infrastructure, to include enhancing its patch and vulnerability management program to address security deficiencies identified during our assessments of NARA’s applications and network infrastructure.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA’s formal written response, we consider this recommendation unresolved and open.

Recommendation 13: Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

8. NARA Must Fully Implement Multi-Factor Authentication

FY 18 FISMA IG Metric Area: *Identity and Access Management*

Multifactor authentication requires two or more credentials when logging on to information systems. Credentials include something you know, such as a password, something you have, like a Personal Identification Verification (PIV) card, or something you are, such as a fingerprint.

However, multi-factor authentication was not fully enforced for NARA non-privileged and privileged users for the majority of FY 2018 as required by NARA IT Security Requirements. Specifically, the roll out of PIV Deployment for non-privileged users was not completed for all associated NARA Libraries until September 2018. Although PIV enforcement was required for elevated privileged NARANet users, it was not enforced for non-NARANet elevated privileged users who had access to other NARA systems.

NARA has missed several previously defined timelines within POA&Ms for PIV implementation due to a lack of adequate project planning and management and technical problems experienced by the implementation contractor.

NARA IT Security Requirements, security control IA-2 for identification and authentication states:

Information systems shall implement multifactor authentication for all data:

- With network access to privileged accounts.
- Requiring moderate or high confidentiality, for network access to non-privileged accounts. Requiring moderate or high confidentiality, for local access to privileged accounts.
- Requiring high confidentiality, for local access to non-privileged accounts.
- The information system shall accept and electronically verifies PIV credentials.

Without full deployment of multi-factor authentication for user accounts, there is an increased risk of unauthorized access to NARA systems.

Recommendation

To assist NARA in continuing to strengthen user authentication controls, CLA recommends the CIO:

Recommendation 14: Ensures multi-factor authentication is enforced for all users with (a) network access via privileged accounts, (b) network access to data requiring moderate or high confidentiality; and/or (c) local access to non-privileged accounts or data, which require high confidentiality.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

9. NARA Must Strengthen Account Management Controls

FY 18 FISMA IG Metric Area: *Identity and Access Management*

Account management controls limit inappropriate access to information systems, protecting the agency's data from unauthorized modification, loss, and disclosure. For account management controls to be effective, they must be consistently implemented and monitored.

Controls were not adequate to ensure NARA performed effective account management for seven of the sampled systems. Specifically, CLA noted the following account management control weaknesses:

- Separated employees retained active accounts on NAC, ISE GSS (e.g., Archives Records Center Information System (ARCIS), Case Management and Reporting System (CMRS) Holdings Management System (HMS)) and NARANet systems.
 - Several of these individuals also logged into the ARCIS, CMRS and HMS systems after separation.
- Individuals were identified on the ISE GSS (e.g., ARCIS, CMRS, and HMS), NAC, OpsPlanner, URTS and NARANet system who did not log in to the system for more than 90 days and were not disabled in accordance with NARA policy.
- Individuals were identified with active user accounts on the ISE GSS (e.g., ARCIS, CMRS), OpsPlanner, URTS and NARANet systems who never logged in and the creation date was greater than 365 days.
- Since the last login date was not captured by the system for Maximo users, CLA was unable to validate whether these users were disabled after 90 days of inactivity.
- The ISSON user access request process was not formalized until February 2018, and user account reviews did not evaluate whether users were currently employed by NARA and still required access to ISSON.
- A review of user access to RRS, Maximo, OpsPlanner, and NAC was not performed during FY 2018 to determine the reasonableness of user access.
- Access request forms and Rules of Behavior (ROB) acknowledgements were not provided for the entire population of sampled ISE GSS, NAC, Ops Planner, and Maximo users.

The noted applications either did not have the capability to automatically disable accounts after 90 days of inactivity, or this particular setting was not properly configured to disable accounts. As a result, IT Security Support Staff (ISS) must perform a manual review of accounts, which is susceptible to error. Additionally, ISSOs are responsible for ensuring all user accounts have been approved by the system owner and there is a User Access Request Form on file for each user account

and to perform user access reviews. They also must track User Access Request Forms and keep them up to date. However, many NARA systems lacked an ISSO for the entire FY.¹³

NARA IT Security Requirements, security control AC-2 for account management states:

- “For data requiring moderate or high confidentiality, the information system automatically disable inactive accounts after [a period not to exceed 90 days for unclassified information systems or 30 days for classified information systems].
- While automated mechanisms do not currently exist that automatically disable system-level accounts, IMO/NITTSS has a user account management SOP that has alternate procedures for reviewing and disabling accounts that have not been used in both 90 and 180 days.
- Additionally, NARA shall authorize access to the information system based on a valid access authorization, intended system usage; and other attributes as required by the system functions.”

NARA IT Security Requirements, security control AC-6 for least privilege states:

- “For data requiring moderate or high confidentiality, the NARA System Owner employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with NARA missions and business functions.”

NARA Cybersecurity Framework Methodology: Processes & Procedures states:

- “For all data, the NARA’s Security Management Division (BX) verifies that Individuals requiring access to information must be screened (e.g., verification of background checks and investigations as well as security and non-disclosure agreements) prior to being granted access. NARA users (both government staff and contractor) are not provided a NARA badge until BX verifies completion of a background check. NARA users are not granted access to systems prior to this screening. Access to systems must be documented through access request forms and approved by system owners.”

Without proper management of user accounts and effective access controls, management cannot accurately determine whether user accounts still require access leading to an increased risk of unauthorized access to the system, data loss, data manipulation, and system unavailability. Inactive accounts that are not disabled in accordance with Agency policy and user accounts that are not disabled when employees separate may be used to gain access to the Agency’s data and sensitive information. In addition, the lack of comprehensive periodic account reviews can lead to system users with greater access than is required to perform their job functions and/or segregation of duties issues.

¹³ Ibid. footnote 4.

Recommendations

To assist NARA in continuing to strengthen the identification and authorization controls, CLA recommends the CIO:

Recommendation 15: Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 16: Ensure upon termination of employment, all system access is disabled in accordance with the applicable system security plan defined period, as described under control PS-4 "Personnel Termination."

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 17: Ensure user access request forms are retained for each user account on all systems.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

10. NARA Must Enforce Elevated Security Training

FY 18 FISMA IG Metric Area: *Security Training*

Agencies should provide Individuals with security roles and responsibilities such as enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level soft

technical training specifically tailored for their assigned duties. This training should be provided before authorizing access to the information system or performing their assigned duties, and repeated on a regular basis.

CLA identified 21 of 126 (17%) active elevated privilege users who did not complete their role-based training by the scheduled completion date and retained system access. NARA relies on a manual process to disable accounts for users that did not complete their training timely, which is susceptible to errors and delays in disabling user access. In addition, there was a lack of management oversight and follow up to ensure training was completed in a timely manner.

NARA's IT Security Methodology for Awareness and Training, states:

- a. "Role-based security-related training is provided to personnel with assigned security roles and responsibilities, within the following groups:
 - **System Administrators** – Entrusted with a high degree of authority over support operations critical to a successful security program, these individuals need a higher degree of technical knowledge in effective security practices and implementation.
 - **System Owners (SOs)** – Must have a broad understanding of security policy and a high degree of understanding regarding security controls and requirements applicable to the systems they manage.
 - **ISSOs** – Act as expert consultants for the agency and therefore must be well educated on security policy and accepted best practices.
 - **IT Security Support Staff [ISM, ISS]** – Develop security policy, standards, and processes for NARA professional/technical staff and those personnel who have been to support NARA mission.
- b. Before authorizing access to the information system or performing assigned duties;
 - All new users with elevated privileges must complete an initial security awareness training by reading the system rules of behavior prior to being issued a system account. Once the new user has completed the security awareness training, the account is made permanent.
- c. System owners/ISSOs are responsible for ensuring system users with elevated privileges complete security awareness training on pertinent security changes made when major system changes occur effecting the system security controls implemented. Failure to complete the training by the specified completion date results in their system account being disabled until the awareness training has been completed. System owners/ISSOs are, also, responsible for notifying IT Security regarding training results and account status.
- d. All NARA users with elevated privileges are required to take pertinent FedVTE training. Failure of users to complete the annual FedVTE security awareness training by the specified completion date results in their system accounts being disabled until the awareness training has been taken."

By not completing role-based training, users may not understand their specific job responsibilities. Additionally, role based training helps elevated users better understand the effects of vulnerabilities and security threats. Without proper training, elevated users are at risk of not being able to identify and remediate security threats leaving NARA systems susceptible to unauthorized access and modification of data.

Recommendation

To assist NARA in continuing to strengthen the elevated privileged user training controls, CLA recommends the Chief Information Officer:

Recommendation 18: Ensure individuals assigned elevated privileges have their user accounts disabled if they have not completed their security awareness training by their scheduled completion date.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA’s formal written response, we consider this recommendation unresolved and open.

11. NARA Must Consistently Implement Audit Logging Procedures

FY 18 FISMA IG Metric Area: *Identity and Access Management*

An audit log is a document to record a security event, determined by an agency, for an information system. Audit logs are a detective control because their trails provide evidence of user activity (user logging in, number failed attempt logon, password reset, etc.).

CLA identified weaknesses in NARA’s audit logging processes. Specifically:

- [REDACTED]
- [REDACTED].

This occurred because Information Services did not provide the appropriate oversight to ensure there was enough capacity to retain [REDACTED] as required by NARA IT Security requirements. In addition, [REDACTED] and system specific policies and procedures were not defined to handle audit logging due to a lack of adequate management oversight.

NARA IT Security Requirements, security control AU-11 for audit record retention states, “for all data, the NARA Office of Information Services shall retain audit records for [a minimum of 1 year for unclassified information, a minimum of 5 years for Sensitive Compartmented Information] to provide support for after-the-fact investigations of security incidents and to meet regulatory and NARA information retention requirements.”

Without adequate collection and monitoring of audit logs, NARA is at risk of not being able to maintain comprehensive organization-wide situational awareness. Limited storage capacity could prevent NARA from conducting effective after-the-fact investigations of security incidents.

Recommendations

To assist NARA in strengthening its audit logging processes, CLA recommends the CIO:

Recommendation 19: Increase NARANet storage capacity to enable the retention of NARANet events in accordance with NARA policy.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 20: Ensure audit logging is enabled for each major information system.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 21: Ensure periodic reviews of generated audit logs are performed for each major information system.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

12. NARA Must Strengthen Password Policies and Shared Account Management

FY 18 FISMA IG Metric Area: *Identity and Access Management*

User authentication is the process of verifying the identity of a user, process, or device, often as a prerequisite for allowing access to resources in an information system. Agencies employ passwords, tokens, or biometrics to authenticate user identities, or in the case of multifactor authentication, a combination thereof. Access to agency information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Agencies may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

NARA’s user authentication controls were not consistently implemented for all information systems. Specifically, CLA identified the following:

- [REDACTED]
- [REDACTED]
- [REDACTED] did not enforce complexity requirements, and lacked configuration of password history requirements.

The [REDACTED] allowed utilization of shared accounts to quickly process researchers in order to cut down long wait times at the NARA registration desk. Similarly, the [REDACTED] did not ensure compliance with NARA’s password policy. Upon notification, management took action to strengthen [REDACTED] password configurations.

NARA IT Security Requirements, security control IA-5 for authentication management states:

“For all data, the NARA Office of Information Services shall manage information system authenticators by (applicable portions only included):

- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Changing/refreshing authenticators [not to exceed 90 days for unclassified information systems or 180 days for classified information systems];
- Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- Changing authenticators for group/role accounts when membership to those accounts changes;
- Enforcing minimum password complexity of [a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each]; and
- Prohibit password reuse for [a minimum of 5 for unclassified information systems or 10 for classified information systems] generations.”

The use of accounts with weak password settings increases the risk of unauthorized access to NARA’s data. In addition, without changing passwords to shared accounts when a user no longer requires system access, the system is susceptible to potential unauthorized access and malicious use and activity.

Recommendations

To assist NARA in strengthening its user authentication controls, CLA recommends the CIO:

Recommendation 22: Ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 23: Ensure the use of shared/group accounts is restricted to only those users with a valid business justification, by enhancing user account review procedures to incorporate reviews of shared/group account membership and reasonableness.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 24: Ensure a process is developed, documented and implemented to change passwords whenever users within shared/group accounts change.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Security Function: Respond

13. NARA Must Report Security Incidents in a Timely Manner

FY 18 FISMA IG Metric Area: *Incident Response*

Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

CLA determined that one of eight total security incidents identified by the NARA Information Services Computer Security Incident Response Team (CSIRT) during 10/1/17 – 3/28/18 was not reported to US-CERT within one hour of discovery in accordance with the NARA IT Security Methodology for Incident Response. As a result, due to management oversight, not all security incidents were reported in accordance with NARA policy.

NARA IT Security Methodology - Incident Response, states:

“NARA shall notify US-CERT of a computer security incident when the confidentiality, integrity, or availability of a NARA information system has been identified to be potentially compromised, with the required data elements, as well as any other available information, within one hour of being identified by the CSIRT.”

Without the timely creation and reporting of security incidents, NARA is at risk of not remediating or mitigating potential threats or incidents in reasonable timeframes and is subject to further exploits of NARA systems.

Recommendation

To assist NARA in strengthening the audit review, analysis and reporting process, CLA recommends the CIO:

Recommendation 25: Ensure incidents are reported to US-CERT within one hour of being identified by the CSIRT of all computer security incidents involving a NARA Information system, in accordance with NARA IT security requirements.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA’s formal written response, we consider this recommendation unresolved and open.

Security Function: Recover

14. NARA Must Develop, Maintain, and Test Contingency Plans

FY 18 FISMA IG Metric Area: *Contingency Planning*

Contingency plans for information systems are utilized to identify essential missions and business functions with associated contingency requirements, and address maintaining essential missions and business functions despite an information system disruption, compromise or failure among other things. These plans need to be updated regularly and tested to ensure recovery procedures are still current and working as intended.

CLA identified several weaknesses in NARA's contingency planning process related to contingency plan development, updates, and testing. Specifically, we noted the following:

- Contingency plans were not developed or finalized for RRS, URTS, OpsPlanner, and Maximo.
- The contingency plan for ISSON was not in place for the entire FY 2018.
- Contingency plans were not tested during FY 2018 for RRS, NAC, OpsPlanner, Maximo and URTS.
- The contingency plan for NAC was last updated in May 2017, lacking annual updates.

These weaknesses existed due to management not scheduling and the CIO not ensuring the annual and complete testing of contingency plans. In addition, many NARA systems lacked an ISSO for the entire FY, who are typically responsible for performing continuous monitoring functions such as updating, developing and testing contingency plans.¹⁴

NARA IT Security Methodology - Contingency Planning, states:

System contingency plans should utilize the NARA Information System Contingency Planning template. This template specifies the following components within contingency plans:

- Identification of essential missions, business functions and associated contingency requirements;
- Provides recovery objectives, restoration priorities, and metrics;
- Describes contingency roles, responsibilities, assigned individuals with contact information;
- Describes how essential missions and business functions will be maintained despite an information system disruption, compromise, or failure;
- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
- Is reviewed and approved by [designated officials within the NARA Security Staff].

NARA IT Security Methodology - Contingency Planning states that for all data, the NARA System Owner or ISSO shall "test the contingency plan for the information system [at least annually] to determine the effectiveness of the plan and the NARA System Owner or ISSOs readiness to execute the plan; review the contingency plan test results; and initiate corrective actions, if needed."

Without a contingency plan, there is a risk that system interruptions and disasters could occur resulting in data recovery efforts not being performed in a timely manner along with the risk that NARA may be unable to recover some of its data. Thus, user access to data could be delayed beyond identified recovery time objectives. In addition, without the regular testing, review, and update of contingency plans, there is an increased likelihood that contact information, software and hardware details and restoration procedures may become outdated and not relevant in the event of a disaster and activation of the plan. This could create a delay in the timely restoration of critical business functions, systems or processes subsequent to a disaster.

¹⁴ Ibid. footnote 4.

Recommendations

To assist NARA in strengthening its contingency planning controls, CLA recommends the CIO:

Recommendation 26: Develop, update and finalize information system contingency plans for all NARA systems.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Recommendation 27: Test the contingency plans for all NARA systems to include documentation of test plans, results and any needed updates to the contingency plan, and establish controls to ensure annual testing of contingency plans.

Management Response

NARA verbally concurs with this recommendation.

OIG Analysis

Until management decision is reached and the OIG receives NARA's formal written response, we consider this recommendation unresolved and open.

Appendix I – Scope and Methodology

Scope

CLA conducted this audit in accordance with performance auditing standards, as specified in the Government Accountability Office’s *Generally Accepted Government Auditing Standards*. Those standards require the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective. The objective of this performance audit was to determine whether NARA implemented an effective information security program in accordance with federal requirements and guidelines. The audit included the testing of selected management, technical, and operational controls outlined in NIST SP 800-53, Revision 4.

CLA assessed NARA’s performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Personnel Security
- Planning
- Privacy
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Service Acquisition

For this audit, selected controls related to the FY2018 IG FISMA reporting metrics from 10 of NARA’s approximately 60 information systems were reviewed. See Appendix IV for a summary of results of each control reviewed.

The audit fieldwork was performed at National Archives II in College Park, MD, from June 1, 2018 to October 15, 2018.

Methodology

To determine if NARA implemented an effective information security program, CLA tested the effectiveness of security controls for a representative subset of agency FISMA reportable systems. This determination in coordination with discussions between OIG and CLA, was risk based using information such as system type (e.g., cloud based, internal or contractor hosted), whether previously audited and FIPS 199 rating of confidentiality, integrity and availability. CLA conducted interviews with NARA officials and contractors, and reviewed legal and regulatory requirements

stipulated in FISMA. Also, documents supporting the information security program were reviewed. These documents included, but were not limited to, NARA's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; and (5) change control documentation. Where appropriate, we compared documents, such as NARA's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, tests of system processes were performed to determine the adequacy and effectiveness of those controls.

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk, and the significance or criticality of the specific items in achieving the related control objectives, was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected, and if projected, may be misleading.

Appendix II – Acronyms

AO	Authorizing Official
ARCIS	Archives Records Center Information System
ATO	Authorization to Operate
CFM	NARA Cybersecurity Framework Methodology
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CLA	CliftonLarsonAllen LLP
CMRS	Case Management and Reporting System
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FTE	Full Time Equivalent
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
HMS	Holdings Management System
IG	Inspector General
ISE GSS	Integrated Siebel Platform General Support System
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISSON	Information Security System Operation Network
IT	Information Technology
NAC	National Archives Catalog
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OFAS	Order Fulfillment and Accounting System
OIG	Office of Inspectors General
OMB	Office of Management and Budget
PIV	Personal Identification Verification
PM	Program Management
POA&M	Plan of Action and Milestones
RCPBS	Records Center Program Billing System
RMF	Risk Management Framework
ROB	Rules of Behavior
RRS	Researcher Registration System
SAISO	Senior Agency Information Security Officer
SAR	Security Assessment Report
SO	System Owner
SP	Special Publication
SSP	System Security Plan
URTS	Unclassified Redaction Tracking System

Appendix III – Management Response

As of the date of this report, we had not received Management's formal response. Upon receipt, we will work with the agency to resolve the recommendations.

Appendix IV - Summary of Results of Each Control Reviewed

The following table identifies NARA systems and controls selected for testing, in addition to the effectiveness of the control.

Control	Control Name	Is Control Effective?
Governance		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AR-1	Governance and Privacy Program	No, See Finding #3
AT-1	Security Awareness and Training Policy and Procedures	No, See Finding #3
CA-1	Security Assessment and Authorization Policies and Procedures	No, See Finding #3 and #4
PM-5	Information System Inventory	No, See Finding #2
PM-7	Enterprise Architecture	Yes
PM-9	Risk Management Strategy	Yes
PM-11	Mission / Business Process Definition	Yes
PM-12	Insider Threat Program	Yes
PS-6	Access Agreements	Yes
IR-1	Incident Response Policy and Procedures	No, See Finding #3
IR-4	Incident Handling	No, See Finding #13
IR-6	Incident Reporting	No, See Finding #13
PM- 8	Critical Infrastructure Plan	Yes
NARANet		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	No, See Finding #9
AC-8	System Use Notification	Yes
AC-17	Remote Access	No, See Finding #8
AR-2	Privacy Impact and Risk Assessment	Yes
AT-1	Security Awareness and Training Policy and Procedures	No, See Finding #3
AT-2	Security Awareness Training	Yes
AT-3	Role-Based Security Training	No, See Finding #10
AT-4	Security Training Records	Yes
CA-2	Security Assessments	No, See Finding #1
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestone	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CA-7	Continuous Monitoring	No, See Finding #1

Control	Control Name	Is Control Effective?
CM-1	Configuration Management Policy and Procedures	No, See Finding #3
CM-2	Baseline Configuration	No, See Finding #6
CM-3	Configuration Change Control	No, See Finding #5
CM-6	Configuration Settings	No, See Finding #6
CM-7	Least Functionality	Yes
CM-8	Information System Component inventory	No, See Finding #2
CM-9	Configuration Management Plan	Yes
CM-10	Software Usage predication	Yes
CP-1	Contingency Planning Policy & Procedures	No, See Finding #3
CP-2	Contingency Plan	Yes
CP-3	Contingency Training	Yes
CP-4	Contingency Plan Testing	Yes
CP-6	Alternate Storage Site	Yes
CP-7	Alternate Processing Sites	Yes
CP-8	Telecommunications Services	Yes
CP-9	Information System Backup	Yes
IA-1	Identification and Authentication Policy and Procedures	No, See Finding #3
IA-3	Device Identification and Authentication	No, See Finding #8
PL-2	System Security Plan	No, See Finding #1
PL-4	Rules of Behavior	Yes
PL-8	Information System Architecture	Yes
PS-1	Personnel Security Policy and Procedures	No, See Finding #3
PS-2	Position Risk Designation	Yes
PS-3	Personnel Screening	Yes
RA-1	Risk Assessment Policy and Procedures	No, See Finding #3
RA-2	Security Categorization	Yes
SA-3	System Development Life	Yes
SA-4	Acquisitions Process	Yes
SA-8	Security Engineering Principles	Yes
SC-12	Cryptographic Key Establishment and Management	No, See Finding #8
SE-2	Privacy Incident Response	Yes
SI-2	Flaw Remediation	No, See Finding #7
SI-4	Information System Monitoring	Yes
RCPBS		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	Yes

Control	Control Name	Is Control Effective?
AR-2	Privacy Impact and Risk Assessment	Yes
CA-2	Security Assessments	No, See Finding #1
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CM-3	Configuration Change Control	Yes
CM-9	Configuration Management Plan	Yes
CP-1	Contingency Planning Policy & Procedures	No, See Finding #3
CP-2	Contingency Plan	Yes
CP-4	Contingency Plan Testing	Yes
CP-6	Alternate Storage Site	Yes
CP-7	Alternate Processing Sites	Yes
PL-2	System Security Plan	No, See Finding #1
PL-4	Rules of Behavior	Yes
OFAS		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	Yes
AR-2	Privacy Impact and Risk Assessment	Yes
CA-2	Security Assessments	No, See Finding #1
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CM-3	Configuration Change Control	Yes
CM-9	Configuration Management Plan	Yes
CP-1	Contingency Planning Policy & Procedures	No, See Finding #3
CP-2	Contingency Plan	Yes
CP-4	Contingency Plan Testing	Yes
CP-6	Alternate Storage Site	Yes
CP-7	Alternate Processing Sites	Yes
PL-2	System Security Plan	No, See Finding #1
PL-4	Rules of Behavior	Yes
ISE GSS		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	No, See Finding #9
AC-8	System Use Notification	Yes
AC-17	Remote Access	No, See Finding #8

Control	Control Name	Is Control Effective?
AR-2	Privacy Impact and Risk Assessment	Yes
AT-3	Role-Based Security Training	Yes
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	Yes
CM-2	Baseline Configuration	No, See Finding #6
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	No, See Finding #6
CM-8	Information System Component Inventory	No, See Finding #2
CM-9	Configuration Management Plan	Yes
CM-10	Software Usage predication	Yes
CP-1	Contingency Planning Policy & Procedures	No, See Finding # 3
CP-2	Contingency Plan	No, See Finding #14
CP-4	Contingency Plan Testing	Yes
CP-7	Alternate Processing Sites	Yes
IA-1	Identification and Authentication Policy and Procedures	No, See Finding #3
IA-3	Device Identification and Authentication	No, See Finding #8
PL-2	System Security Plan	No, See Finding #1
PL-4	Rules of Behavior	Yes
SC-12	Cryptographic Key Establishment and Management	No, See Finding #8
ISSON		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	No, See Finding #9
AR-2	Privacy Impact and Risk Assessment	Yes
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CM-3	Configuration Change Control	Yes
CP-2	Contingency Plan	No, See Finding #14
CP-4	Contingency Plan Testing	Yes
CP-7	Alternate Processing Sites	Yes
PL-2	System Security Plan	No, See Finding #1
NAC		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	No, See Finding #9
AR-2	Privacy Impact and Risk Assessment	Yes

Control	Control Name	Is Control Effective?
AT-3	Role-Based Security Training	Yes
CA-2	Security Assessments	No, See Finding #1
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CP-2	Contingency Plan	No, See Finding #14
CP-4	Contingency Plan Testing	No, See Finding #14
IA-1	Identification and Authentication Policy and Procedures	No, See Finding #3
RRS		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	No, See Finding #9
AR-2	Privacy Impact and Risk Assessment	Yes
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	Yes
CM-3	Configuration Change Control	Yes
CP-2	Contingency Plan	No, See Finding #14
CP-4	Contingency Plan Testing	No, See Finding #14
CP-7	Alternate Processing Sites	Yes
PL-2	System Security Plan	No, See Finding #1
OpsPLANNER		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	No, See Finding #9
AR-2	Privacy Impact and Risk Assessment	Yes
CA-2	Security Assessments	No, See Finding #1
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CP-2	Contingency Plan	No, See Finding #14
CP-4	Contingency Plan Testing	No, See Finding #14
CP-7	Alternate Processing Sites	Yes
IA-1	Identification and Authentication Policy and Procedures	No, See Finding #3
PL-2	System Security Plan	No, See Finding #1
MAXIMO		
AC-1	Access Control Policy & Procedures	No, See Finding #3

Control	Control Name	Is Control Effective?
AC-2	Account Management	No, See Finding #9, 11 and 12
AR-2	Privacy Impact and Risk Assessment	Yes
AT-3	Role-Based Security Training	Yes
CA-2	Security Assessments	No, See Finding #1
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CM-3	Configuration Change Control	Yes
CP-2	Contingency Plan	No, See Finding #14
CP-4	Contingency Plan Testing	No, See Finding #14
CP-7	Alternate Processing Sites	Yes
PL-2	System Security Plan	No, See Finding #1
URTS		
AC-1	Access Control Policy & Procedures	No, See Finding #3
AC-2	Account Management	No, See Finding #11
AR-2	Privacy Impact and Risk Assessment	Yes
AT-3	Role-Based Security Training	Yes
CA-3	System interconnections	Yes
CA-5	Plan of Action and Milestones	No, See Finding #1
CA-6	Security Accreditation	No, See Finding #1
CM-3	Configuration Change Control	Yes
CP-2	Contingency Plan	No, See Finding #14
CP-4	Contingency Plan Testing	No, See Finding #14
CP-6	Alternate Storage Site	Yes
CP-7	Alternate Processing Sites	Yes
PL-2	System Security Plan	No, See Finding #1

Appendix V – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Deputy Chief Operating Officer
Chief of Management and Administration
Chief Information Officer
Accountability
Government Accountability Office
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

OIG Hotline

To report fraud, waste, or abuse, please contact us:

Electronically:

[OIG Hotline Referral Form](#)

Telephone:

301-837-3500 (Washington, D.C. Metro Area)

1-800-786-2551 (toll-free and outside the Washington, D.C. metro area)

Mail:

IG Hotline

NARA

P.O. Box 1821

Hyattsville, MD 20788-0821

Office of Inspector General’s Assessment of Management’s Response and Proposed Actions

The *Audit of National Archives and Records Administration’s Compliance with the Federal Information Security Modernization Act* (Audit Report No. 19-AUD-02) was issued by CLA on December 14, 2018 with NARA’s verbal agreement to the 27 recommendations documented in the report. On December 19, 2018, the OIG received *Management’s Response* to CLA’s Report and a summary of their proposed actions. NARA concurred with all 27 recommendations. We assessed management’s response and proposed actions and consider NARA’s proposed actions responsive to CLA’s recommendations. All of the recommendations will remain open and resolved pending completion of the corrective actions.

Finding 1, Recommendations 1 - 6

To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO:

Recommendation 1: Ensure complete security authorization packages for each major application and general support system¹ are completed prior to deployment into production.

Management Response

Information Services will revise NARA 804, IT Systems Security, and NARA 805, Systems Development Life Cycle, to establish additional controls to ensure each new major application and general support system (GSS) has a completed security authorization package before deployment to production. Information Services will complete authorization packages and re-authorize systems that are currently operating without security authorization.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA’s proposed action responsive to CLA’s recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 2: Ensure SSPs are developed for all NARA systems in accordance with NARA policy.

Management Response

Information Services will develop System Security Plans (SSP) for all systems that are currently lacking them. This action depends on contracted Information Systems Security Officer (ISSO) resources that were acquired in 1Q FY 2019; the target completion date

¹ OMB Circular A-130, Appendix III, defines general support system as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

reflects time necessary for ISSOs to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 3: Ensure SSPs are reviewed and updated for all NARA systems in accordance with NARA policy to ensure any missing control implementation details are completed, and missing privacy controls added.

Management Response

Information Services will conduct a comprehensive review of SSPs for all NARA systems and update, correct, or complete missing data, as needed. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 4: Conduct risk assessments for each system in operation and establish policies or procedures to ensure that risk assessments are conducted at least annually.

Management Response

Information Services will revise NARA 804, IT Systems Security, to establish additional controls to ensure that system risk assessments are conducted at least annually. Information Services, with ISSO support, will conduct risk assessments for all systems at least annually.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 5: Document summaries of test failures for all failed controls identified in Security Assessment Reports.

Management Response

Information Services will update guidance on preparing Security Assessment Reports to ensure the reports document summaries of failed test controls and countermeasures for failed controls.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 6: Ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated timely; and are updated to include detailed information on the status of the corrective actions.

Management Response

Information Services will work with information system owners to review all system POA&Ms and update as needed to ensure they include target completion dates; are remediated in a timely manner; and include detailed information on the status of the corrective actions. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 2, Recommendation 7

To assist NARA with strengthening its system inventory controls, CLA recommends the CIO:

Recommendation 7: Ensure the system inventory listing is updated to accurately reflect NARA's current operating environment.

Management Response

Information Services will review and update its system inventory listing to ensure it accurately reflects NARA's current operating environment.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 3, Recommendation 8

To assist NARA with strengthening its policy and procedure development and authorization controls, CLA recommends the Chief Information Officer in coordination with Strategy and Performance staff:

Recommendation 8: Ensure IT policies, procedures, methodologies and supplements are reviewed and approved in accordance with NARA Directive 111.

Management Response

In coordination with Strategy and Performance, Information Services will update NARA Directive 804 and its associated supplements, in accordance with NARA Directive 111.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 4, Recommendation 9

To assist NARA with strengthening its ISSO management controls, CLA recommends the CIO:

Recommendation 9: Assign ISSO's for all major applications and general support systems.

Management Response

Information Services will assign an ISSO for all major applications and general support systems.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 5, Recommendation 10

To assist NARA with strengthening its change management controls, CLA recommends the Chief Information Officer:

Recommendation 10: Ensure that all applicable changes are tested and properly approved before being implemented into production, with evidence maintained of testing and approvals.

Management Response

Information Services will ensure testing of applicable Requests for Change (RFCs) are approved by the Enterprise Change Advisory Board prior to implementation. Information Services will also maintain evidence of testing and approvals. Cases where the only real test is when the change is made in the production environment (e.g. a DNS change) will be documented in the RFC.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 6, Recommendation 11

To assist NARA with strengthening its baseline configuration management controls, CLA recommends the CIO:

Recommendation 11: Ensure reviews of baseline configurations are performed on an annual basis and updated as necessary.

Management Response

Information Services will review baseline configurations on an annual basis, and update as necessary.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 7, Recommendations 12 - 13

To assist NARA with strengthening its vulnerability management controls, CLA recommends the CIO:

Recommendation 12: Implement improved processes to remediate security deficiencies on NARA's network infrastructure, to include enhancing its patch and vulnerability management program to address security deficiencies identified during our assessments of NARA's applications and network infrastructure.

Management Response

Information Services will update its patch and vulnerability management process to ensure consistent and timely remediation of security deficiencies and will continue to remediate issues as they arise.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 13: Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.

Management Response

Information Services will ensure all information systems migrate away from unsupported operating systems, including Windows Server 2003, to vendor-supported operating systems.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 8, Recommendation 14

To assist NARA in continuing to strengthen user authentication controls, CLA recommends the CIO:

Recommendation 14: Ensures multi-factor authentication is enforced for all users with (a) network access via privileged accounts, (b) network access to data requiring moderate or high confidentiality; and/or (c) local access to non-privileged accounts or data, which require high confidentiality.

Management Response

To the extent possible, Information Services will continue implementation of multi-factor authentication for NARANet for all users with network access via privileged accounts, and for data requiring moderate confidentiality.

The plan is to further implement 2-factor authentication to applications on the network requiring moderate or high confidentiality. Local access to non-privileged accounts or data residing on the network and requiring high confidentiality will be accomplished through the implementation of 2-factor authentication of applications.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. However, the OIG will need to be provided with documented explanation on the qualifier "to the extent possible," in case Information Services could only partially fulfill the recommendation as stated. Such documentation should include: (1) why Information Services could not fully implement the recommendation; and (2) the solution(s) Information Services utilized in attempt to fully implement the recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 9, Recommendations 15 - 17

To assist NARA in continuing to strengthen the identification and authorization controls, CLA recommends the CIO:

Recommendation 15: Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.

Management Response

Information Services will ensure that ISSOs are periodically reviewing accounts to ensure timely disabling of accounts when required. NARA is in the process of implementing Privileged Management (PRIVMGMT) as part of the DHS CDM initiative. The capability for automated disabling of privileged accounts will then be implemented.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 16: Ensure upon termination of employment, all system access is disabled in accordance with the applicable system security plan defined period, as described under control PS-4 “Personnel Termination.”

Management Response

NARA will update NARA Directive 215, Exit Clearance Procedures, to ensure that Information Services receives timely notification of employee separations and reassignments. Information Services will work with the Office of Human Capital to ensure, upon termination of employment, all system access is disabled in accordance with the applicable system security plan defined period, as described under control PS-4 “Personnel Termination”.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA’s proposed action responsive to CLA’s recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 17: Ensure user access request forms are retained for each user account on all systems.

Management Response

Information Services will retain user account request forms on all systems.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA’s proposed action responsive to CLA’s recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 10, Recommendation 18

To assist NARA in continuing to strengthen the elevated privileged user training controls, CLA recommends the Chief Information Officer:

Recommendation 18: Ensure individuals assigned elevated privileges have their user accounts disabled if they have not completed their security awareness training by their scheduled completion date.

Management Response

Information Services will update NARA 804, IT Systems Security, to require that user accounts with elevated privileges are disabled if the account holder has not completed their security awareness training by their scheduled completion date.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 11, Recommendations 19 - 21

To assist NARA in strengthening its audit logging processes, CLA recommends the CIO:

Recommendation 19: Increase NARANet storage capacity to enable the retention of NARANet events in accordance with NARA policy.

Management Response

Information Services will increase the storage capacity available for its Tenable Log Correlation Engine (LCE) audit log storage and correlation solution to ensure sufficient capacity exists to maintain logs for at least 1 year.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 20: Ensure audit logging is enabled for each major information system.

Management Response

Information Services will ensure audit logging is enabled for each major information system.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 21: Ensure periodic reviews of generated audit logs are performed for each major information system.

Management Response

Information Services will assign an ISSO for each major information system and ensure ISSOs perform weekly audit log reviews. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 12, Recommendations 22 -24

To assist NARA in strengthening its user authentication controls, CLA recommends the CIO:

Recommendation 22: Ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements.

Management Response

Information Services will ensure password configuration settings for all major information systems, including RRS and Maximo, are in accordance with NARA IT Security Requirements.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 23: Ensure the use of shared/group accounts is restricted to only those users with a valid business justification, by enhancing user account review procedures to incorporate reviews of shared/group account membership and reasonableness.

Management Response

Information Services will work with the System Owner to ensure the use of shared/group accounts is restricted to only those users with a valid business justification and will review shared user accounts at least annually.

Target Completion Date: December 31, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 24: Ensure a process is developed, documented and implemented to change passwords whenever users within shared/group accounts change.

Management Response

The System ISSO/Owner will develop, document, and implement a process to change passwords within shared/group accounts, when users change.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 13, Recommendation 25

To assist NARA in strengthening the audit review, analysis and reporting process, CLA recommends the CIO:

Recommendation 25: Ensure incidents are reported to US-CERT within one hour of being identified by the CSIRT of all computer security incidents involving a NARA Information system, in accordance with NARA IT security requirements.

Management Response

Information Services will ensure incidents are reported to US-CERT within one hour of being identified by the CSIRT of all computer security incidents involving a NARA information system, in accordance with NARA IT security requirements.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 14, Recommendations 26 -27

To assist NARA in strengthening its contingency planning controls, CLA recommends the CIO:

Recommendation 26: Develop, update and finalize information system contingency plans for all NARA systems.

Management Response

Information Services will assign an ISSO for each information system who will develop and document Information Security Contingency Plan (ISCP) for each information system. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target

completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 27: Test the contingency plans for all NARA systems to include documentation of test plans, results and any needed updates to the contingency plan, and establish controls to ensure annual testing of contingency plans.

Management Response

Information Services will assign an ISSO for each information system who will ensure the ISCP for each information system includes documentation of test plans, as well as results and any needed updates to the contingency plan. Information Services will also establish additional controls to ensure annual testing of contingency plans. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

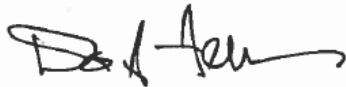
Management Response



Date: 19 December 2018
To: James Springs, Inspector General
From: David S. Ferriero, Archivist of the United States
Subject: Management's Response to OIG Report 19-AUD-02, *Audit of NARA's Compliance with the Federal Information Security Modernization Act – Fiscal Year 2018*

Thank you for the opportunity to provide comments on this final report. We appreciate your willingness to meet and clarify language in the report.

We concur with the 27 recommendations in this audit, and in response, the attachment provides a summary of our proposed actions. As each recommendation is satisfied, we will provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.



DAVID S. FERRIERO
Archivist of the United States

Attachment

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Action Plan Response to OIG Report 19-AUD-02,

*Audit of NARA's Compliance with the Federal Information Security
Modernization Act*

Recommendation 1: To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure complete security authorization packages for each major application and general support system are completed prior to deployment into production.

Planned Action: Information Services will revise NARA 804, *IT Systems Security*, and NARA 805, *Systems Development Life Cycle*, to establish additional controls to ensure each new major application and general support system (GSS) has a completed security authorization package before deployment to production. Information Services will complete authorization packages and re-authorize systems that are currently operating without security authorization.

Target Completion Date: October 30, 2020

Recommendation 2: To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure SSPs are developed for all NARA systems in accordance with NARA policy.

Planned Action: Information Services will develop System Security Plans (SSP) for all systems that are currently lacking them. This action depends on contracted Information Systems Security Officer (ISSO) resources that were acquired in 1Q FY 2019; the target completion date reflects time necessary for ISSOs to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

Recommendation 3: To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure SSPs are reviewed and updated for all NARA systems in accordance with NARA policy to ensure any missing control implementation details are completed, and missing privacy controls added.

Planned Action: Information Services will conduct a comprehensive review of SSPs for all NARA systems and update, correct, or complete missing data, as needed. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

Recommendation 4: To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO conduct risk assessments for each system in operation and establish policies or procedures to ensure that risk assessments are conducted at least annually.

Planned Action: Information Services will revise NARA 804, *IT Systems Security*, to establish additional controls to ensure that system risk assessments are conducted at least annually. Information Services, with ISSO support, will conduct risk assessments for all systems at least annually.

Target Completion Date: October 30, 2020

Recommendation 5: To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO document summaries of test failures for all failed controls identified in Security Assessment Reports.

Planned Action: Information Services will update guidance on preparing Security Assessment Reports to ensure the reports document summaries of failed test controls and countermeasures for failed controls.

Target Completion Date: September 30, 2019

Recommendation 6: To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated timely; and are updated to include detailed information on the status of the corrective actions.

Planned Action: Information Services will work with information system owners to review all system POA&Ms and update as needed to ensure they include target completion dates; are remediated in a timely manner; and include detailed information on the status of the corrective actions. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

Recommendation 7: To assist NARA with strengthening its system inventory controls, CLA recommends the CIO ensure the system inventory listing is updated to accurately reflect NARA's current operating environment.

Planned Action: Information Services will review and update its system inventory listing to ensure it accurately reflects NARA's current operating environment.

Target Completion Date: September 30, 2019

Recommendation 8: To assist NARA with strengthening its policy and procedure development and authorization controls, CLA recommends the CIO, in coordination with Strategy and Performance staff, ensure IT policies, procedures, methodologies and supplements are reviewed and approved in accordance with NARA Directive 111.

Planned Action: In coordination with Strategy and Performance, Information Services will update NARA Directive 804 and its associated supplements, in accordance with NARA Directive 111.

Target Completion Date: September 30, 2019

Recommendation 9: To assist NARA with strengthening its ISSO management controls, CLA recommends the CIO assign ISSO's for all major applications and general support systems.

Planned Action: Information Services will assign an ISSO for all major applications and general support systems.

Target Completion Date: September 30, 2019

Recommendation 10: To assist NARA with strengthening its change management controls, CLA recommends the CIO ensure that all applicable changes are tested and properly approved before being implemented into production, with evidence maintained of testing and approvals.

Planned Action: Information Services will ensure testing of applicable Requests for Change (RFCs) are approved by the Enterprise Change Advisory Board prior to implementation. Information Services will also maintain evidence of testing and approvals. Cases where the only real test is when the change is made in the production environment (e.g. a DNS change) will be documented in the RFC.

Target Completion Date: September 30, 2019

Recommendation 11: To assist NARA with strengthening its baseline configuration management controls, CLA recommends the CIO ensure reviews of baseline configurations are performed on an annual basis and updated as necessary.

Planned Action: Information Services will review baseline configurations on an annual basis, and update as necessary.

Target Completion Date: September 30, 2019

Recommendation 12: To assist NARA with strengthening its vulnerability management controls, CLA recommends the CIO implement improved processes to remediate security deficiencies on NARA's network infrastructure, to include enhancing its patch and vulnerability management program to address security deficiencies identified during our assessments of NARA's applications and network infrastructure.

Planned Action: Information Services will update its patch and vulnerability management process to ensure consistent and timely remediation of security deficiencies and will continue to remediate issues as they arise.

Target Completion Date: September 30, 2019

Recommendation 13: To assist NARA with strengthening its vulnerability management controls, CLA recommends the CIO ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.

Planned Action: Information Services will ensure all information systems migrate away from unsupported operating systems, including Windows Server 2003, to vendor-supported operating systems.

Target Completion Date: September 30, 2019

Recommendation 14: To assist NARA in continuing to strengthen user authentication controls, CLA recommends the CIO ensures multi-factor authentication is enforced for all users with (a) network access via privileged accounts, (b) network access to data requiring moderate or high confidentiality; and/or (c) local access to non-privileged accounts or data, which require high confidentiality.

Planned Action: To the extent possible, Information Services will implement multi-factor authentication for NARANet for all users with network access via privileged accounts, and for data requiring moderate confidentiality.

Information Services has completed the implementation of 2-factor authentication for network access via privileged accounts at the end of FY18. The plan is to further implement 2-factor authentication to applications on the network requiring moderate or high confidentiality. Local access to non-privileged accounts or data residing on the network and requiring high confidentiality will be accomplished through the implementation of 2-factor authentication of applications.

Target Completion Date: October 30, 2020

Recommendation 15: To assist NARA in continuing to strengthen the identification and authorization controls, CLA recommends the CIO ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.

Planned Action: Information Services will ensure that ISSOs are periodically reviewing accounts to ensure timely disabling of accounts when required. NARA is in the process of implementing Privileged Management (PRIVMGMT) as part of the DHS CDM initiative. The capability for automated disabling of privileged accounts will then be implemented.

Target Completion Date: October 30, 2020

Recommendation 16: To assist NARA in continuing to strengthen the identification and authorization controls, CLA recommends the CIO ensure upon termination of employment, all system access is disabled in accordance with the applicable system security plan defined period, as described under control PS-4 "Personnel Termination."

Planned Action: NARA will update NARA Directive 215, Exit Clearance Procedures, to ensure that Information Services receives timely notification of employee separations and reassignments. Information Services will work with the Office of Human Capital to ensure, upon termination of employment, all system access is disabled in accordance with the applicable system security plan defined period, as described under control PS-4 "Personnel Termination".

Target Completion Date: September 30, 2019

Recommendation 17: To assist NARA in continuing to strengthen the identification and authorization controls, CLA recommends the CIO ensure user access request forms are retained for each user account on all systems.

Planned Action: Information Services will retain user account request forms on all systems.

Target Completion Date: September 30, 2019

Recommendation 18: To assist NARA in continuing to strengthen the elevated privileged user training controls, CLA recommends the CIO ensure individuals assigned elevated privileges have their user accounts disabled if they have not completed their security awareness training by their scheduled completion date.

Planned Action: Information Services will update NARA 804, *IT Systems Security*, to require that user accounts with elevated privileges are disabled if the account holder has not completed their security awareness training by their scheduled completion date.

Target Completion Date: September 30, 2019

Recommendation 19: To assist NARA in strengthening its audit logging processes, CLA recommends the CIO increase NARANet storage capacity to enable the retention of NARANet events in accordance with NARA policy.

Planned Action: Information Services will increase the storage capacity available for its Tenable Log Correlation Engine (LCE) audit log storage and correlation solution to ensure sufficient capacity exists to maintain logs for at least 1 year.

Target Completion Date: March 29, 2019

Recommendation 20: To assist NARA in strengthening its audit logging processes, CLA recommends the CIO ensure audit logging is enabled for each major information system.

Planned Action: Information Services will ensure audit logging is enabled for each major information system.

Target Completion Date: October 30, 2020

Recommendation 21: To assist NARA in strengthening its audit logging processes, CLA recommends the CIO ensure periodic reviews of generated audit logs are performed for each major information system.

Planned Action: Information Services will assign an ISSO for each major information system and ensure ISSOs perform weekly audit log reviews. This action depends on contracted ISSOs that were acquired in 1Q FY 2019; the target completion date reflects time necessary to organize and learn NARA systems, before performing the work associated with this action.

Target Completion Date: October 30, 2020

Recommendation 22: To assist NARA in strengthening its user authentication controls, CLA recommends the CIO ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements.

Planned Action: Information Services will ensure password configuration settings for all major information systems, including RRS and Maximo, are in accordance with NARA IT Security Requirements.

Target Completion Date: October 30, 2020

Recommendation 23: To assist NARA in strengthening its user authentication controls, CLA recommends the CIO ensure the use of shared/group accounts is restricted to only those users with a valid business justification, by enhancing user account review procedures to incorporate reviews of shared/group account membership and reasonableness.

Planned Action: Information Services will work with the System Owner to ensure the use of shared/group accounts is restricted to only those users with a valid business justification and will review shared user accounts at least annually.

Target Completion Date: December 31, 2019

Recommendation 24: To assist NARA in strengthening its user authentication controls, CLA recommends the CIO ensure a process is developed, documented and implemented to change passwords whenever users within shared/group accounts change.

Planned Action: The System ISSO/Owner will develop, document, and implement a process to change passwords within shared/group accounts, when users change.

Target Completion Date: October 30, 2020

Recommendation 25: To assist NARA in strengthening the audit review, analysis and reporting process, CLA recommends the CIO ensure incidents are reported to US-CERT within one hour of being identified by the CSIRT of all computer security incidents involving a NARA information system, in accordance with NARA IT security requirements.